

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of pro-actively refreshing credentials by an entity that maintains credentials, the method comprising:

- a) determining credentials that are required to access resources including resource-specific constraints that indicate when the credentials must be refreshed;
- ab) storing in a memory, a profile collection having at least one credential profile, each credential profile including a credential, resource-specific constraints for the credential and related information; and
- bc) for each credential profile in the profile collection:
 - i) in accordance with at least one criterion of a refresh policy and prior to a time of presentation of the credential, making a determination, from that credential profile's ~~related information~~ resource-specific constraints, of whether that credential needs to be refreshed so that, at the time of presentation, that credential will meet the resource-specific constraints;
 - ii) replacing the stored credential with a new credential in the credential profile if the stored credential does need to be refreshed; and
 - iii) updating the related information of the new credential in the credential profile.

2. (Previously Presented) The method of claim 1, wherein the method further comprises creating the profile collection by, for each of at least one needed credential, determining whether the profile collection includes a credential profile for needed credentials, and, if not, then:

5 creating an empty credential profile;
6 gathering that needed credential;
7 storing that needed credential in the credential profile;
8 obtaining related information including resource constraints on that
9 needed credential; and
10 storing the information in the credential profile.

1 3. (Previously Presented) The method of claim 2, wherein the resource constraints
2 are obtained by manual entry of a user.

1 4. (Previously Presented) The method of claim 2, wherein the resource constraints
2 are deduced through access attempts.

1 5. (Previously Presented) The method of claim 2, wherein the resource constraints
2 are obtained from a directory.

1 6. (Previously Presented) The method of claim 2, wherein the constraints are
2 obtained from a resource server.

1 7. (Original) The method of claim 2, wherein the stored credential includes a public
2 key identity credential.

1 8. (Original) The method of claim 2, wherein the stored credential includes a group
2 membership credential.

1 9. (Original) The method of claim 2, wherein the stored credential includes a group
2 non-membership credential.

1 10. (Original) The method of claim 2, wherein the stored credential includes a non-
2 revocation credential.

- 1 11. (Original) The method of claim 2, wherein the stored resource constraints include
2 a recency requirement.
- 1 12. (Original) The method of claim 2, wherein the stored resource constraints include
2 a trust level.
- 1 13. (Original) The method of claim 2, wherein the stored resource constraints include
2 a maximum credential chain length.
- 1 14. (Previously Presented) The method of claim 1, wherein the related information
2 includes a credential identifier.
- 1 15. (Previously Presented) The method of claim 1, wherein the related information
2 includes when the credential was issued.
- 1 16. (Previously Presented) The method of claim 1, wherein the related information
2 includes when the credential was last used for a resource access.
- 1 17. (Previously Presented) The method of claim 1, wherein the related information
2 includes information on the resource on which the credential was last used.
- 1 18. (Previously Presented) The method of claim 1, wherein at least one said criterion
2 is such that the method includes refreshing credentials that are older than a
3 certain time period.
- 1 19. (Previously Presented) The method of claim 1, wherein at least one said criterion
2 is such that the method includes refreshing credentials that were last used within
3 a certain time period.

1 20. (Previously Presented) The method of claim 1, wherein at least one said criterion
2 is such that the method includes refreshing credentials that are older than an
3 associated recency requirement.

1 21. (Previously Presented) The method of claim 1, wherein at least one said criterion
2 is such that the method includes refreshing credentials that are predicted to be
3 used in a next session.

1 22. (Currently Amended) A processor readable medium having instructions
2 contained therein which when executed by a processor causes the processor to
3 execute a method of pro-actively refreshing credentials by an entity that
4 maintains credentials, the method comprising:

5 a) determining credentials that are required to access resources including
6 resource-specific constraints that indicate when the credentials must be
7 refreshed;

8 ab) storing in a memory, a profile collection having at least one credential
9 profile, each credential profile including a credential, resource-specific
10 constraints for the credential and related information; and

11 bc) for each credential profile in the profile collection:

12 i) in accordance with at least one criterion of a refresh policy and prior
13 to a time of presentation of the credential, making a determination,
14 from that credential profile's ~~related information~~ resource-specific
15 constraints, of whether that credential needs to be refreshed so
16 that, at the time of presentation, that credential will meet the
17 resource-specific constraints;

18 ii) replacing the stored credential with a new credential in the
19 credential profile if the stored credential needs to be refreshed; and

20 iii) updating the related information of the new credential in the
21 credential profile.

- 1 23. (Previously Presented) The processor readable medium of claim 22 wherein the
2 method further comprises creating the profile collection for each of at least one
3 needed credential determining whether the profile collection includes a credential
4 profile for that needed credential, and, if not, then
5 creating an empty credential profile;
6 gathering that needed credential;
7 storing that needed credential in the credential profile;
8 obtaining related information including resource constraints on that
9 needed credential; and
10 storing the information in the credential profile.
- 1 24. (Previously Presented) The processor readable medium of claim 23, wherein the
2 resource constraints are obtained by manual entry of a user.
- 1 25. (Previously Presented) The processor readable medium of claim 2 wherein
2 resource constraints are obtained by deducing them through access attempts.
- 1 26. (Previously Presented) The processor readable medium of claim 2 wherein
2 resource constraints are obtained from a directory.
- 1 27. (Previously Presented) The processor readable medium of claim 2 wherein
2 resource constraints are from a resource server.
- 1 28. (Previously Presented) The processor readable medium of claim 2 wherein the
2 stored credential includes a public key identity credential.
- 1 29. (Previously Presented) The processor readable medium of claim 2 wherein the
2 stored credential includes a group membership credential.
- 1 30. (Previously Presented) The processor readable medium of claim 2 wherein the
2 stored credential includes a group non-membership credential.

- 1 31. (Previously Presented) The processor executable readable medium of claim 2.
2 wherein the stored credential includes a non-revocation credential.
- 1 32. (Previously Presented) The processor readable medium of claim 2 wherein the
2 stored resource constraints include a recency requirement.
- 1 33. (Previously Presented) The processor readable medium of claim 2 wherein the
2 stored resource constraints include a trust level.
- 1 34. (Previously Presented) The processor readable medium of claim 23, wherein the
2 stored resource constraints include a maximum credential chain length.
- 1 35. (Previously Presented) The processor executable-readable medium of claim 2
2 wherein the related information includes a credential identifier.
- 1 36. (Previously Presented) The processor readable medium of claim 21 wherein the
2 related information includes information on when the credential issued.
- 1 37. (Previously Presented) The processor readable medium of claim 2 wherein the
2 related information includes information on when the credential last used for a
3 resource access.
- 1 38. (Previously Presented) The processor readable medium of claim 2 wherein the
2 related information includes information on the resource on the resource on the
3 credential was last used.
- 1 39. (Previously Presented) The processor readable medium of claim 2 wherein at
2 least one said criterion is such that the method includes refreshing credentials
3 that are older than a certain time period.

1 40. (Previously Presented) The processor readable medium of claim 2 wherein at
2 least one said criterion is such that the method includes refreshing credentials
3 that were last used within a certain time period.

1 41. (Previously Presented) The processor readable medium of claim 2 wherein at
2 least one said criterion is such that the method includes refreshing credentials
3 that are older than an associated recency requirement.

1 42. (Previously Presented) The processor executable readable medium of claim 2
2 wherein at least one said criterion is such that the method includes refreshing
3 credentials that are predicted to be used in a next session.

1 43. (Currently Amended) A system for pro-actively refreshing credentials by an entity
2 that maintains credentials, the system comprising:

3 a mechanism that determines credentials that are required to access
4 resources including resource-specific constraints that indicate when the
5 credentials must be refreshed;

6 a memory to store a profile collection having at least one credential profile,
7 each credential profile including a credential, resource-specific constraints for the
8 credential and related information;

9 a circuit to read the credential profile;

10 a refresh policy stored in the memory to determine prior to a time of
11 presentation of the credential, if the credential needs to be refreshed using the
12 related information resource-specific constraints so that, at the time of
13 presentation, that credential will meet the resource-specific constraints, wherein
14 the circuit replaces the stored credential with a new credential in the credential
15 profile if the stored credential needs to be refreshed and the circuit updates the
16 related information of the new credential in the credential profile.

1 44. (Previously Presented) The system of claim 43, wherein the circuit is configured
2 to determine, for each of at least one needed credential, whether the profile

3 collection includes a credential profile for that needed credential, and, if not, then
4 create an empty credential profile in the memory, gather that needed credential;
5 store that needed credential in the credential profile; obtain related information
6 including resource constraints on that needed credential, and store the
7 information in the credential profile.

1 45. (Original) The system as in claim 44, wherein the circuit is a processor.

1 46. (Previously Presented) The system of claim 44, wherein the resource constraints
2 are obtained by manual entry of a user.

1 47. (Previously Presented) The system of claim 44, wherein the resource constraints
2 are deduced through access attempts.

1 48. (Previously Presented) The system of claim 44, wherein the resource constraints
2 are obtained from a directory.

1 49. (Previously Presented) The system of claim 44, wherein the resource constraints
2 are obtained from a resource server.

1 50. (Original) The system of claim 44, wherein the stored credential includes a public
2 key identity credential.

1 51. (Original) The system of claim 44, wherein the stored credential includes a group
2 membership credential.

1 52. (Original) The system of claim 44, wherein the stored credential includes a group
2 non-membership credential.

1 53. (Original) The system of claim 44, wherein the stored credential includes a non-
2 revocation credential.

- 1 54. (Original) The system of claim 44, wherein the stored resource constraints
2 include a recency requirement.
- 1 55. (Original) The system of claim 44, wherein the stored resource constraints
2 include a trust level.
- 1 56. (Original) The system of claim 44, wherein the stored resource constraints
2 include a maximum credential chain length.
- 1 57. (Previously Presented) The system of claim 43, wherein the related information
2 includes a credential identifier.
- 1 58. (Previously Presented) The system of claim 43, wherein the related information
2 includes when the credential was issued.
- 1 59. (Previously Presented) The system of claim 43, wherein the related information
2 includes when the credential was last used for a resource access.
- 1 60. (Previously Presented) The system of claim 43, wherein the related information
2 includes on which resource the credential was last used.
- 1 61. (Original) The system of claim 43, wherein the refresh policy refreshes
2 credentials that are older than a certain time period.
- 1 62. (Original) The system of claim 43, wherein the refresh policy refreshes
2 credentials that were last used within a certain time period.
- 1 63. (Original) The system of claim 43, wherein the refresh policy refreshes
2 credentials that are older than an associated recency requirement.

- 1 64. (Original) The system of claim 43, wherein the refresh policy refreshes
- 2 credentials that are predicted to be used in a next session.